

# Complex Reflection Group Coding

Hye Jung Kim

Thesis Committee:  
Dr. J.B. Nation, Adviser  
Dr. Ralph Freese

Graduate Committee:  
Dr. Michelle Manes  
Dr. Monique Chyba  
Dr. Robert Little

# Acknowledgements

I would like to thank my adviser, Dr. J.B. Nation, for being persistent and patient with me for the past two years. At times, I took two steps forward and three steps back and Dr. Nation was incredibly patient with me all the time. I would also like to thank all the professors who provided me with loads of knowledge in numerous areas of mathematics. I truly enjoyed all the classes that I was offered at the University of Hawaii at Manoa. Special thank you to Dr. Manabu Hagiwara, for granting me an opportunity to travel to Japan and to present my research to numerous professors and corporate leaders. I would like to thank SUPER-M for providing me with the two years of experience in the K-12 classrooms and making me realize where my passion and future lie. Last, but definitely not the least, I would like to thank my friends and family for always being so supportive of me and for always helping me find my way in numerous areas of life.

## Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
<b>2</b>	<b>Preliminaries</b>	<b>5</b>
2.1	Linear Algebra . . . . .	5
2.2	Reflection Groups . . . . .	6
<b>3</b>	<b>Subgroup Decoding</b>	<b>7</b>
3.1	Example: G25 Subgroup Decoding . . . . .	8
<b>4</b>	<b>Description of the New Algorithm</b>	<b>10</b>
<b>5</b>	<b>General Decoding Algorithm</b>	<b>12</b>
<b>6</b>	<b>Issues in Decoding</b>	<b>15</b>
<b>7</b>	<b>Future Research</b>	<b>15</b>

# Complex Reflection Group Coding

Hye Jung Kim

March 28, 2011

## Abstract

This paper considers complex reflection groups for which the generalization of subgroup decoding method does not work at all are considered in this paper. A new method of decoding is introduced to effectively encode and decode the exceptional complex reflection groups. A general decoding algorithm is devised and the results of analysis are presented. Discussion of future research is presented as well.

## 1 Introduction

In 1968, Slepian introduced the idea of group codes using groups of orthogonal matrices for the Gaussian channel [1]. Afterwards, in 1996, Mittelholzer and Lahtonen published a comprehensive paper on real reflection group coding and an efficient decoding algorithm [3]. This was further refined by W. Wesley Peterson, J.B. Nation, and Marc Fosserier [4].

Regardless of the difference of geometry, Kim, Nation, and Shepler [5] extended the method described in [4] to codes based on certain complex reflection groups. For this paper, we address decoding algorithms for group codes based on other types of complex reflection groups. We will use the classifications of finite unitary groups generated by reflections as determined by Shephard and Todd [6]. The subgroup coding method [4] works well for a large class of groups including  $G(r, 1, n)$ ,  $G(r, k, n)$  and also some exceptional groups such as G4, G8, and G16 but without error correction properties as mentioned in [5]. However, the method does not work at all for some other exceptional complex reflection groups such as G25 and G26.

The goal of this paper is to develop methods of encoding and decoding that will work effectively for group codes using groups for which the subgroup decoding method fails. The paper also includes

an analysis of why the basic type of decoding scheme works whenever the noise is sufficiently small.

## 2 Preliminaries

In this section we introduce definitions and notations that are used throughout the paper. Also included in this section are proofs of specific properties that arise and will be used.

### 2.1 Linear Algebra

To make this paper self-contained, we present some definitions in linear algebra along with highlighted properties. The conjugate transpose of any matrix  $M$  will be denoted  $M^H$ .

**Definition 2.1.** A *unitary matrix*  $U$  is a square matrix such that  $UU^H = I$ . In other words,  $U^H = U^{-1}$ .

If the entries of the matrix are real, then unitary matrices are simply orthogonal matrices.

**Definition 2.2.** The *standard inner product*,  $\langle \vec{x}, \vec{y} \rangle$ , is defined to be  $\vec{x}^H \vec{y}$ .

With this definition, we can show a useful property that will be referred to in the following sections.

**Proposition 2.3.** Let  $M$  be an  $n \times n$  unitary matrix and  $\vec{x}, \vec{y}$  be vectors in an  $n$ -dimensional vector space. Then  $\langle M\vec{x}, \vec{y} \rangle = \langle \vec{x}, M^H \vec{y} \rangle$

*Proof.* We have

$$\begin{aligned} \langle M\vec{x}, \vec{y} \rangle &= (M\vec{x})^H \vec{y} \\ &= \vec{x}^H M^H \vec{y} \\ &= \langle \vec{x}, M^H \vec{y} \rangle \end{aligned}$$

□

**Definition 2.4.** A *unitary group* is a group of  $n \times n$  unitary matrices with the usual matrix multiplication operation.

**Proposition 2.5.** A unitary group acting on an  $n$ -dimensional vector space preserves the standard inner product,  $\langle \vec{x}, \vec{y} \rangle = \vec{x}^H \vec{y}$ . Moreover, a unitary matrix is an isometry on a vector space.

*Proof.* Let  $\mathbf{G}$  be a unitary group and  $g \in \mathbf{G}$  and  $\vec{x}, \vec{y}$  be elements of the  $n$ -dimensional vector space. Then

$$\begin{aligned}\langle g\vec{x}, g\vec{y} \rangle &= (g\vec{x})^H g\vec{y} \\ &= \vec{x}^H g^H g\vec{y} \\ &= \vec{x}^H \vec{y} \\ &= \langle \vec{x}, \vec{y} \rangle\end{aligned}$$

Hence  $\langle g\vec{x}, g\vec{y} \rangle = \langle \vec{x}, \vec{y} \rangle$  for all elements of the unitary group.

Now we need to show that  $g$  is an isometry. Define distance as

$$\begin{aligned}d(\vec{x}, \vec{y}) &\equiv ||\vec{x} - \vec{y}|| \\ &= \sqrt{|x_1 - y_1|^2 + \cdots + |x_n - y_n|^2} \\ &= \sqrt{(x - y)^H (x - y)} \\ &= \sqrt{\langle x - y, x - y \rangle}.\end{aligned}$$

So  $d(g\vec{x}, g\vec{y}) = \sqrt{\langle g(x - y), g(x - y) \rangle} = \sqrt{\langle x - y, x - y \rangle} = d(\vec{x}, \vec{y})$ , hence  $g$  is an isometry.  $\square$

## 2.2 Reflection Groups

Now we proceed with definitions and properties regarding reflection groups. In this paper, only complex reflection groups are considered.

**Definition 2.6.** A *reflection* is an isometry on a vector space that fixes a hyperplane.

**Definition 2.7.** A *reflection group* is a group of unitary matrices that is generated by a set of reflections.

Every complex reflection can be represented algebraically as a linear transformation:

$$S(\vec{y}) = \vec{y} + (\lambda - 1)\langle \vec{\alpha}, \vec{y} \rangle \vec{\alpha},$$

where  $\vec{\alpha}$  is a vector of unit length, and  $\lambda$  is a complex number of modulus 1. We can relate the above algebraic expression to the real reflection by setting  $\lambda$  to be  $-1$ .

**Proposition 2.8.** *Conjugating a reflection by any group element yields another reflection.*

*Proof.* Let  $S$  be a reflection and  $g \in \mathbf{G}$  where  $\mathbf{G}$  is a reflection group.

$$\begin{aligned}
gSg^{-1}(\vec{y}) &= gS(g^{-1}(\vec{y})) \\
&= g(g^{-1}\vec{y} + (\lambda - 1)\langle \vec{\alpha}, g^{-1}\vec{y} \rangle \vec{\alpha}) \\
&= gg^{-1}\vec{y} + (\lambda - 1)\langle \vec{\alpha}, g^{-1}\vec{y} \rangle g\vec{\alpha} \\
&= \vec{y} + (\lambda - 1)\langle g\vec{\alpha}, \vec{y} \rangle g\vec{\alpha} \\
&= S'(\vec{y}),
\end{aligned}$$

thus conjugation of reflections by any group element is another reflection.  $\square$

Also, the inverse, or more generally any power, of a reflection is a reflection.

**Definition 2.9.** A *coset leader* is a minimum-length expression of coset representatives.

As mentioned in the introduction, we will use the Shephard and Todd classification of finite unitary groups generated by reflections. The classification consists of  $G(r, p, n)$  which are considered in [5] and 34 exceptional cases numbered 4 – 37. This paper will consider various exceptional groups and the details of the exceptional groups will be discussed in the following sections.

### 3 Subgroup Decoding

Let  $\mathbf{G}$  be a group of isometries acting on a vector space  $\mathbf{V}$ , and fix a point  $\vec{x}_0 \in \mathbf{V}$ . The group code consists of the orbit of  $\vec{x}_0$  under the elements of  $\mathbf{G}$ . The point  $\vec{x}_0$  is called the *initial vector*. In this paper, initial vectors being considered will consist of only real nonzero components.

The set up for subgroup decoding consists of selecting a sequence of reflection subgroups of  $\mathbf{G}$  such that

$$\{I\} = H_0 < H_1 < \cdots < H_{k-1} < H_k = \mathbf{G}.$$

Then find all the distinct coset leaders of  $H_i$  over  $H_{i-1}$  and arrange them as spanning trees of coset leaders. The expression of a group element as a product of coset leaders is the canonical expression for that element. The idea will become more concrete through a detailed example in the following section.

If  $g \in \mathbf{G}$  is the group element corresponding to the message needed to be sent, encode it as  $\vec{x} = g^{-1}\vec{x}_0$ , where  $\vec{x}_0$  is the initial vector. Note that  $g$  can be expressed as a product of coset leaders,  $g = c_k c_{k-1} \dots c_2 c_1$ , so the encoded vector is

$$\vec{x} = c_1^{-1} c_2^{-1} \dots c_{k-1}^{-1} c_k^{-1} \vec{x}_0$$

On the receiving side of the channel,  $\vec{r} = \vec{x} + \vec{n}$  is received, where  $\vec{n}$  is the noise added during the transmission. Decode the received vector by recursively finding a sequence of coset leaders  $d_1, \dots, d_k$  such that for each  $j$ ,  $d_j \dots d_1 \vec{r}$  minimizes the distance to the initial vector  $\vec{x}_0$ . In other words, to find the sequence of coset leaders, we go through the spanning trees of coset leaders and apply reflections so that at each step the vector obtained is closer to  $\vec{x}_0$  in distance. Ideally,  $d_i = c_i$  for  $1 \leq i \leq k$ , but this may not be the case with the addition of the noise. Further details of subgroup decoding are explained in detail in [4].

### 3.1 Example: G25 Subgroup Decoding

The subgroup decoding method is compatible, without satisfying error correction properties [5], with  $G(r, 1, n)$ ,  $G(r, k, n)$  and also some exceptional groups such as G4, G8, and G16. However, it is not compatible with certain other exceptional complex reflection groups. To make the concepts in the previous section more concrete and to show why subgroup decoding is not compatible with some exceptional complex reflection groups as classified by Shephard and Todd [6], take the complex reflection group G25 as an example. G25 consists of 24 reflections and has a total of 648 elements. The following matrices generate the group G25 which lives in three dimensional complex space,  $\mathbb{C}^3$ :

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega \end{pmatrix}, \mathbf{B} = \frac{-i}{\sqrt{3}} \begin{pmatrix} \omega & \omega^2 & \omega^2 \\ \omega^2 & \omega & \omega^2 \\ \omega^2 & \omega^2 & \omega \end{pmatrix}, \mathbf{C} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where  $\omega = e^{\frac{2\pi i}{3}}$ . Note the presentation:  $A^3 = B^3 = C^3 = I, ABA = BAB, CBC = BCB, AC = CA$ . We use the following sequence of subgroups:

$$\{I\} < \langle A \rangle < \langle A, B \rangle < \langle A, B, C \rangle$$

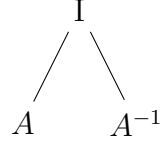


and denote it as

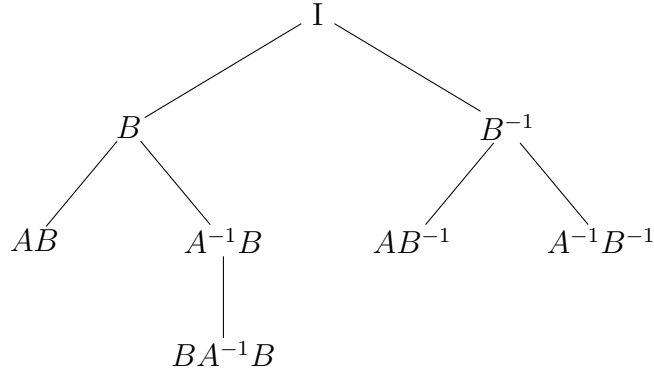
$$H_0 < H_1 < H_2 < H_3.$$

The spanning trees for the coset leader graphs is as follows:

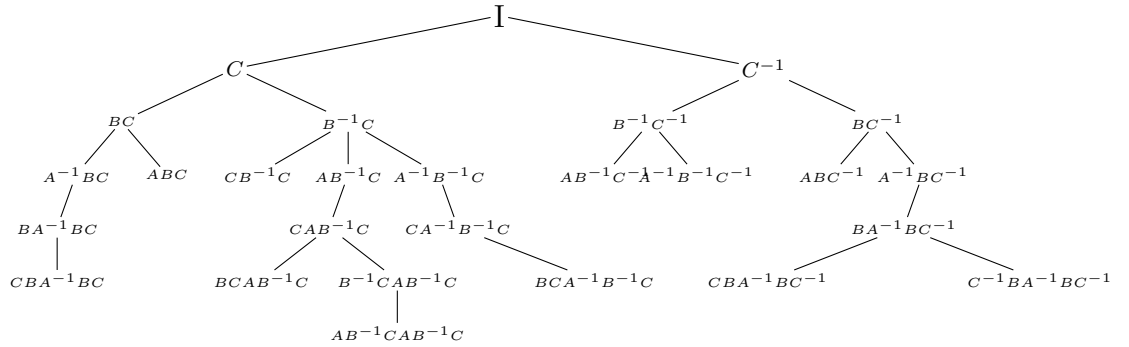
Coset leaders of  $H_1$  over  $H_0$



Coset leaders of  $H_2$  over  $H_1$



Coset leaders of  $H_3$  over  $H_2$



It turns out that subgroup decoding does not work for G25. Set  $\vec{x}_0 = (3, -1, -1)$ . Note that this initial vector is chosen such that  $\|a\vec{x}_0 - \vec{x}_0\| = \|b\vec{x}_0 - \vec{x}_0\| = \|c\vec{x}_0 - \vec{x}_0\|$ . Consider the example

where  $CB^{-1}C = CB^2C$  is the group element corresponding to the message. Note that  $CB^2C$  is a coset leader of  $H_3$  over  $H_2$ . We encode it as  $C^{-1}(B^2)^{-1}C^{-1}\vec{x}_0 = C^2BC^2\vec{x}_0$  and send it through the channel. Even with no noise added during the transmission, when decoding, the coset leader  $B^2$  over  $H_1$  leads to a smaller distance. Overall the decoded vector is  $BC^2B^2$ , which is not equivalent to the message  $CB^2C$ . Statistically, out of the 648 elements of G25, approximately half decode properly to the group element that was sent, depending on the initial vector chosen.

So upon figuring out that the idea did not work in reality, there were numerous attempts to alter certain parameters to see if it would work. Since the initial vector, subgroup sequence, and coset leaders are parameters at our disposal, different combinations of which were attempted, including trying millions of initial vectors.

Subgroup decoding works for the complex permutation groups  $G(r, 1, n)$ ,  $G(r, k, n)$  and for at least some of the exceptional complex reflection groups, including G4, G8, and G16. Whereas there is a slight chance that the perfect combination of these parameters were not found for G25 and G26, it is convincing to think that this subgroup decoding method is not compatible with these exceptional complex reflection groups at all. This is what led to the development of the new method using complex reflection groups which is described in the following section.

## 4 Description of the New Algorithm

The overall communication model is summarized in the following figure:

$$m \xrightarrow{\gamma} g \mapsto g^{-1}\vec{x}_0 \rightarrow \boxed{\text{Channel}} \rightarrow \vec{r} \mapsto g'\vec{r} \mapsto g' \xrightarrow{\gamma^{-1}} m'.$$

The setup consists of picking a particular complex reflection group  $\mathbf{G}$  acting on a vector space  $\mathbf{V} = \mathbb{C}^n$ . For each group element  $g$ , choose a minimal length expression of  $g$  as a product of reflections to be its canonical form. That is, we consider the set of all reflections as a generating set for  $\mathbf{G}$ . Let  $g$  represent a message. Since  $g \in \mathbf{G}$ ,  $g = t_l t_{l-1} \dots t_1$ , where  $t_i$  are reflections in  $\mathbf{G}$ .

We select an initial vector  $\vec{x}_0$  on the unit sphere in  $V$ , and the code consists of  $\mathbf{G}\vec{x}_0 = \{g\vec{x}_0 : g \in \mathbf{G}\}$ . Let  $\gamma : M \rightarrow \mathbf{G}$  denote the

correspondence between the message and the group elements. The details of  $\gamma$  are omitted since it does not affect our formulation.

The message  $\vec{m}$  has the corresponding group element  $g = \gamma(\vec{m})$ . Encode the message by applying  $g^{-1}$  to  $\vec{x}_0$ . So the message being sent is  $\vec{x} = g^{-1}\vec{x}_0 = t_1^{-1} \dots t_{l-1}^{-1} t_l^{-1} \vec{x}_0$ . The received vector has the form  $\vec{r} = \vec{x} + \vec{n}$  where  $\vec{n}$  is the channel noise.

Now decode iteratively by finding the sequence of reflections  $s_1, \dots, s_n$  such that, for each  $k$ ,  $\vec{h}_k = s_k \dots s_2 s_1 \vec{r}$  maximizes the real part of the dot product  $\langle \vec{h}, \vec{x}_0 \rangle$  where  $\vec{h}$  is all the combination of  $k$  reflections applied to  $\vec{r}$ . So the overall product of the sequence,  $g' = s_n \dots s_2 s_1$  maximizes the dot product  $\langle \vec{h}, \vec{x}_0 \rangle$  where  $\vec{h}$  runs over all combinations of  $k$  or fewer reflections applied to  $\vec{r}$ . Note the following theorem:

**Theorem 4.1.** *Maximizing the real part of the dot product is equivalent to minimizing the distance between the sequence applied to the received vector and the initial vector.*

*Proof.* Let  $\vec{z} = (z_1, z_2, \dots, z_n)$  denote the received vector with the sequence of reflections applied to it and  $\vec{x} = (x_1, x_2, \dots, x_n)$  denote the initial vector. The distance can be calculated as follows:

$$\begin{aligned} \|\vec{z} - \vec{x}\|^2 &= \|(z_1, z_2, \dots, z_n) - (x_1, x_2, \dots, x_n)\|^2 \\ &= \|(z_1 - x_1, z_2 - x_2, \dots, z_n - x_n)\|^2 \\ &= |z_1 - x_1|^2 + |z_2 - x_2|^2 + \dots + |z_n - x_n|^2 \\ &= \{|z_1|^2 + |x_1|^2 - 2\text{Re}(z_1)x_1 + |z_2|^2 + |x_2|^2 - 2\text{Re}(z_2)x_2 + \dots \\ &\quad + |z_n|^2 + |x_n|^2 - 2\text{Re}(z_n)x_n\}. \end{aligned}$$

The last equality is due to the fact that for any complex numbers  $a$  and  $b$ , where  $b$  only has real nonzero components,

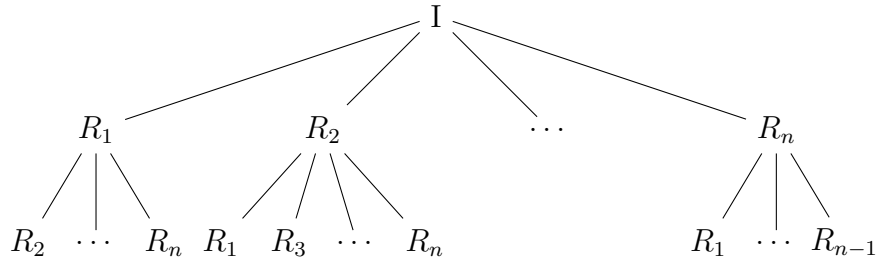
$$\begin{aligned} |a - b|^2 &= (a - b)(\overline{a - b}) \\ &= a\bar{a} - \bar{a}b - a\bar{b} + b\bar{b} \\ &= |a|^2 + |b|^2 - \bar{a}b - ab \\ &= |a|^2 + |b|^2 - (\bar{a} + a)b \\ &= |a|^2 + |b|^2 - 2\text{Re}(a)b. \end{aligned}$$

Since  $b$  only consists of real components,

$$\begin{aligned} \text{Re}\langle a, b \rangle &= \text{Re}\{a^H b\} \\ &= \text{Re}(a)b. \end{aligned}$$

Therefore, by the above calculations, it is clear that minimizing the distance is equivalent to maximizing the dot product.  $\square$

Hence the decoding process can be shown pictorially as follows:



and continuing on until the maximum dot product is achieved. In the upcoming section, the proof will be provided that this process does terminate. Then decode by taking the received message as  $\vec{m}' = \gamma^{-1}(g')$ .

This decoding algorithm can be generalized and this is what leads us to the next section.

## 5 General Decoding Algorithm

In this section the generalization of the previous section is provided. We start off with the generic description of the decoding algorithm. The basic decoding algorithm considered has the following parameters:

- a finite unitary group  $\mathbf{G}$  acting on a vector space  $\mathbf{V}$
- an initial vector  $\vec{x}_0$  of unit length in  $\mathbf{V}$
- an ordered generating set  $X$  for  $\mathbf{G}$ .

The codewords consists of the orbit of the initial vector  $\vec{x}_0$  under the action of  $\mathbf{G}$ , same as in the subgroup decoding case. Every message has a corresponding group element of  $\mathbf{G}$ . Let  $g$  be the corresponding group element. The canonical representation of the group element

is as products of elements of  $X$ . Note that this expression may not be unique. The codeword  $\vec{x} = g^{-1}\vec{x}_0$  is transmitted. The received vector is  $\vec{r} = \vec{x} + \vec{n}$  where  $\vec{n}$  is the noise added during the transmission. Let  $\vec{r}_0 = \vec{r}$ . Given  $\vec{r}_k$ , we can apply the transformation  $c_{k+1} \in X \cup \{I\}$  to obtain  $\vec{r}_{k+1} = c_{k+1}\vec{r}_k$  and then repeat the process. If  $c_{k+1} = I$ , we terminate the process. Note that  $c_{k+1}$  is chosen such that either of the following holds:

- (A)  $c_{k+1}$  minimizes  $\|c_{k+1}\vec{r}_k - \vec{x}_0\|$ ;
- (B)  $c_{k+1}$  is the first such that  $\|c_{k+1}\vec{r}_k - \vec{x}_0\| < \|\vec{r}_k - \vec{x}_0\| - \frac{1}{2}\delta$ , where  $\delta$  is defined as below, and if no such exists, then  $c_{k+1} = I$ .

Note that if we choose  $c_{k+1}$  as in (B), we may decrease the number of checks that are being done.

Note that the generating set  $X$  is arbitrary. For a reflection group  $\mathbf{G}$ , there are two extremes for  $X$ : the minimal generating set, or the set of all reflections. First we investigate if the procedure terminates and decodes correctly.

Let us assume that

( $\dagger$ ) if  $\vec{x}_0 \neq \vec{w} \in \mathbf{G}\vec{x}_0$ , then there exists  $c \in X$  such that  $\|c\vec{w} - \vec{x}_0\| < \|\vec{w} - \vec{x}_0\|$ .

For each codeword  $\vec{w}$ , let

$$C_M(\vec{w}) = \{c \in X \cup \{I\} : \|c\vec{w} - \vec{x}_0\| \text{ is minimal}\}.$$

Note that ( $\dagger$ ) is equivalent to if  $\vec{w} \neq \vec{x}_0$ , then  $I \notin C_M(\vec{w})$ . Define

$$\delta = \min\{\|\vec{w} - \vec{x}_0\| - \|c\vec{w} - \vec{x}_0\|\}$$

where the minimum is taken over all  $\vec{w} \in \mathbf{G}\vec{x}_0 - \vec{x}_0$  and  $c \in C_M(\vec{w})$ .

Now, we have the following theorem that shows that when noise is small, the algorithm terminates and decodes the message properly.

**Theorem 5.1.** *If  $\|\vec{r} - \vec{x}\| < \frac{\delta}{3}$ , then the algorithm terminates in at most  $\lfloor \frac{6}{\delta} \rfloor$  steps with  $c_k \dots c_1 \in g\mathbf{H}$ , where  $\mathbf{H}$  is the stabilizer of  $\vec{x}_0$ .*

*Proof.* The process terminates in at most

$$\frac{\max\|\vec{w} - \vec{x}_0\|}{\frac{\delta}{3}} \leq \frac{6}{\delta}$$

steps, without counting the last step where the identity is chosen. Now that we know that the process terminates, we must show that

it decodes the message properly. It suffices to show that the process does not terminate until  $\|c_n \dots c_1 \vec{r} - \vec{x}_0\| < \frac{\delta}{2}$ , where the assumption  $(\ddagger)$  is useful. At the  $k^{th}$  step, set  $g' = c_k \dots c_1$  and  $\vec{w} = g' \vec{x} = g' g^{-1} \vec{x}_0$  and  $\vec{r}_k = g' \vec{r}$ . If  $\vec{w} = \vec{x}_0$ , we are done. Suppose  $\vec{w} \neq \vec{x}_0$ . Note that  $\|\vec{w} - \vec{r}_k\| < \frac{\delta}{3}$ , since

$$\begin{aligned} \|\vec{r} - \vec{x}\| &= \|\vec{r} - g^{-1} \vec{x}_0\| \\ &= \|g' \vec{r} - g' g^{-1} \vec{x}_0\| \\ &= \|\vec{w} - \vec{r}_k\|. \end{aligned}$$

By  $(\ddagger)$ , since  $\vec{w} \neq \vec{x}_0$ , there exists some  $c \in C_M(\vec{w})$  such that  $\|c\vec{w} - \vec{x}_0\| < \|\vec{w} - \vec{x}_0\|$ . Since

$$\delta = \min\{\|\vec{w} - \vec{x}_0\| - \|c\vec{w} - \vec{x}_0\|\}$$

where the minimum is taken over all  $\vec{w} \in \mathbf{G}\vec{x}_0 - \vec{x}_0$  and  $c \in C_M(\vec{w})$ ,

$$\|c\vec{w} - \vec{x}_0\| + \delta < \|\vec{w} - \vec{x}_0\|.$$

By triangle inequality,

$$\begin{aligned} \|c\vec{r}_k - \vec{x}_0\| &\leq \|c\vec{r}_k - c\vec{w}\| + \|c\vec{w} - \vec{x}_0\| \\ &< \frac{\delta}{3} + \|c\vec{w} - \vec{x}_0\|. \end{aligned}$$

Also,

$$\begin{aligned} \|\vec{r}_k - \vec{x}_0\| &\geq \|\vec{w} - \vec{x}_0\| - \|\vec{r}_k - \vec{w}\| \\ &\geq \|c\vec{w} - \vec{x}_0\| + \delta - \|\vec{r}_k - \vec{w}\| \\ &> \|c\vec{w} - \vec{x}_0\| + \delta - \frac{\delta}{3} \\ &= \|c\vec{w} - \vec{x}_0\| + \frac{2\delta}{3}. \end{aligned}$$

So,

$$\|\vec{r}_k - \vec{x}_0\| > \|c\vec{w} - \vec{x}_0\| + \frac{2\delta}{3},$$

which is the same as

$$\|\vec{r}_k - \vec{x}_0\| - \frac{\delta}{3} > \|c\vec{w} - \vec{x}_0\| + \frac{\delta}{3}.$$

Now, putting it all together, we have

$$\|c\vec{r}_k - \vec{x}_0\| < \frac{\delta}{3} + \|c\vec{w} - \vec{x}_0\| < \|\vec{r}_k - \vec{x}_0\| - \frac{\delta}{3}$$

thus  $c_{k+1}$  is at least  $\frac{\delta}{3}$  closer.  $\square$

Thus we just showed that the new algorithm in the previous section actually terminates and decodes to the correct group element.

## 6 Issues in Decoding

In the real reflection group codes using the subgroup decoding method, the decoding was unique. In the case of complex reflection group codes as defined above, there needs to be a lookup table. This is due to the fact that the representation of group elements, as products of reflections, is generally not unique. The process decodes to a group element that is equal to the group element being sent, however the representation may be different. This arises because of the fact that each group element can be expressed as a product of reflections, but there need not be a unique minimal length expression.

## 7 Future Research

The new algorithm can be improved upon to require fewer checks to decode. There may be further analysis that needs to be done prior to cutting down steps, however, it seems very feasible for the process to be shorter. Also, further analysis and understanding will be needed to see exactly why the subgroup decoding is not compatible with certain exceptional groups while it does work for others. At this point, we are not entirely certain why it does not work, we only are aware that it does not.

## References

- [1] D. Slepian, Group codes for the Gaussian channel, Bell Syst. Tech. J. 47 (1968), 575-602.
- [2] D. Slepian, Permutation modulation, Proc. IEEE, vol. 53, no. 3, pp. 228-236, Mar. 1965

- [3] T. Mittelholzer and J. Lahtonen, Group codes generated by finite reflection groups, *IEEE Trans. on Information Theory*, 42 (1996), 519-528.
- [4] M. Fossorier, J. Nation, and W. Peterson, Reflection group codes and their decoding, *IEEE Transactions on Information Theory*, 56 (2010), 6273-6293.
- [5] H. Kim, J. Nation, and A. Shepler, Complex reflection group codes and their decoding, preprint 2010
- [6] G. C. Shephard and J. A. Todd, Finite unitary reflection groups, *Canadian J. Math.* 6 (1954), 274-304.